We Claim:

1. A method for providing a secure communications session with a user terminal in a communications network, the method comprising the steps of:

transmitting first and second secure keys to the user terminal using a secure communications method, the first and second secure keys being suitable for storage in the user terminal for use during the secure communications session;

encrypting and transmitting data to the user terminal using a current session key, and receiving and decrypting data received from the user terminal using the current session key, the first secure key initially being used as the current session key; and

periodically generating a subsequent session key using the second secure key and using the subsequent session key as the current session key during subsequent communications between the communications network and the user terminal.

2. The method according to claim 1, further comprising the step of:

logging off the user terminal in response to an encrypted logoff request from the user terminal accompanied by the second secure key.

3. The method according to claim 1, wherein the periodically generating step comprises generating the subsequent session key by concatenating the current session key with the second secure key and applying a hash algorithm.

4. A method for providing a secure communications session with a mobile terminal in a wireless local access network (WLAN), the method comprising the steps of:

transmitting first and second secure keys to the mobile terminal using a secure communications method, the first and second secure keys being suitable for storage in the mobile terminal for use during the secure communications session;

encrypting and transmitting data to the mobile terminal using a current session key, and receiving and decrypting data received from the mobile terminal using the current session key, the first secure key initially being used as the current session key; and

periodically generating a subsequent session key using the second secure key and using the subsequent session key as the current session key during subsequent communications with the mobile terminal.

5. The method as in claim 4, wherein the periodically generating step comprises generating a subsequent session key using a combination of a new key and the second secure key, the new key being generated using the first secure key.

6. The method as in claim 5, wherein the periodically generating step comprises generating a subsequent session key by concatenating the new key and the second secure key and running a hash algorithm to generate the subsequent session key.

7. A method for providing a secure communications session with a mobile terminal in a wireless local access network (WLAN), the method comprising the steps of:

generating a secure key;

transmitting the secure key to the mobile terminal using a secure communications method, the secure key being stored in the mobile terminal for use during the secure communications session;

encrypting and transmitting data to the mobile terminal using a current session key, and receiving and decrypting data received from the mobile terminal using the current session key; and

ending the secure communications session in response to receiving a logoff message from the mobile terminal, the logoff message being in encrypted form and including the secure key.

8. A method for providing a secure communications session with a mobile terminal in a wireless local access network (WLAN), the method comprising the steps of:

generating first and second secure keys;

transmitting the first and second secure keys to the WLAN using a secure communications method, the first and second secure keys being stored in the WLAN for use during the secure communications session;

encrypting and transmitting data to the WLAN using a current session key, and receiving and decrypting data received from the WLAN using the current session key, the first secure key initially being used as the current session key; and

periodically generating a subsequent session key using the second secure key and using the subsequent session key as the current session key during subsequent communications with the mobile terminal.

9. The method as in claim 8, wherein the periodically generating step comprises generating a subsequent session key using a combination of a new key and the second secure key, the new key being generated using the first secure key.

10. The method as in claim 9, wherein the periodically generating step comprises generating a subsequent session key by concatenating the new key and the second secure key and running a hash algorithm to generate the subsequent session key.

11. A method for providing a secure communications session with a mobile terminal in a wireless local access network (WLAN), the method comprising the steps of:

generating a secure key;

transmitting the secure key to the WLAN using a secure communications method, the secure key being stored in the WLAN for use during the secure communications session;

encrypting and transmitting data to the WLAN using a current session key, and receiving and decrypting data received from the WLAN using the current session key; and

ending the secure communications session in response to receiving a logoff message from the WLAN, the logoff message being in encrypted form and including the secure key.

12. A method for providing a secure communications session with a mobile terminal in a wireless local access network (WLAN), the method comprising the steps of:

installing at least two shared secrets on both the mobile terminal and the WLAN access point during the user authentication phase whereby a first secret is the initial session key and a second secret is utilized as secure seed to generate subsequent session keys.

13. The method as in claim 12, further comprising the step of generating a new key and encrypting the new key with the current session key and exchanging and the new key between the WLAN and the mobile terminal.

14. The method as in claim 12, further comprising the step of the WLAN and the mobile terminal generating a new session key employing the new session key and the secure seed.

15. The method as in claim 14, wherein generating the new session key generation comprises the step of concatenating the said new key to the secure seed.

16. The method as in claim 15, further comprising the step of generating a new session key by applying a hash algorithm on said concatenated result.

17. The method as in claim 16, further comprising the step of using the said new session key in communication between the WLAN and mobile terminal.

18. A method for providing a secure communications session between a mobile terminal and a wireless local access network (WLAN), the method comprising the steps of:

a mobile terminal sending during session logoff an encrypted logoff request accompanied by the secure seed such that the secure seed appears in the logoff request.

19. An access point for providing a secure communications session between a mobile terminal and a wireless local access network (WLAN), comprising:

a means for transmitting first and second secure keys to the mobile terminal using a secure communications method and

a means to encrypt data using the first secure key and a means to periodically generate a subsequent session key using the second secure key.

20. A terminal device for providing a secure communications session with a communications network, comprising:

a means to receive a first secure key and a second secure key and a means to store the first secure key and the second secure key for use during the secure communications session;

a means to receive data and a means to decrypt the data using a current session key during the secure communications session, the first secure being using initially as the current session key; and

a means to generate a subsequent session key using the current session key and the second secure key, the subsequent session key thereafter being used as the current session key for subsequent communications.

21. The terminal device according to claim 20, wherein the terminal device comprises a mobile terminal and the communications network comprises a wireless local area network (WLAN).

22. The access point for providing a secure communications session between a mobile terminal and a wireless local access network (WLAN) in claim 20, wherein the means to periodically generate a subsequent session key comprises a means to generate a subsequent session key using a combination of a new key and the second secure key, the new key being generated by means using the first secure key.

23. The access point for providing a secure communications session between a mobile terminal and a wireless local access network (WLAN) in claim 20, wherein the means to periodically generate a subsequent session key comprises a means to generate a subsequent session key by concatenating the new key and the second secure key and a means for running a hash algorithm to generate the subsequent session key.